JOURNAL OF ALGEBRA 135, 381–387 (1990)

On a Characterization of Algebraic Number Fields with Class Number Less than Three

SCOTT T. CHAPMAN*

Department of Mathematics, Trinity University, 715 Stadium Drive, San Antonio, Texas 78212

AND

WILLIAM W. SMITH

Department of Mathematics, The University of North Carolina at Chapel Hill, Chapel Hill, North Carolina 27599-3250

Communicated by A. Fröhlich

Received October 24, 1988

A well known theorem of L. Carlitz states that classical algebraic number fields have class number less than or equal to two if and only if any two factorizations of an algebraic integer into irreducible elements contains the same number of factors. We show that the same result holds using a somewhat weaker factorization condition. This leads to a characterization of Dedekind domains with class number less than or equal to three. © 1990 Academic Press, Inc.

In [1] L. Carlitz shows that a finite algebraic number field over the rationals has class number less than or equal to two if and only if any two factorizations of an integer into irreducibles contains the same number of irreducible factors. This result has spawned much work in commutative algebra and algebraic number theory. In [13], Zaks considers integral domains in general with this property and calls them half factorial domains (HFD). His paper [12] contains an extensive study of such domains. The papers [4, 5, 7–10] all contain arithmetic characterizations of rings of algebraic integers with class numbers bigger than two and [11] contains a study of some factorization properties of these same rings. The purpose of this note is to show that Carlitz' original condition on the factorization can

* The first author received support under the John M. Bennett Fellowship at Trinity University and also gratefully acknowledges the support of The University of North Carolina at Chapel Hill.

0021-8693/90 $3.00

be changed to a weaker condition which continues to characterize these domains. This condition leads further to a characterization of Dedekind domains in general with class number less than or equal to three.

To begin, we restate Carlitz's result using Zaks' terminology.

THEOREM. *Let D be the ring of integers of a finite algebraic number field K over the rationals. Then K has class number less than or equal to two if and only if D is a HFD.*

Consider the following generalization of a half factorial domain.

DEFINITION. Let D be an integral domain. D is a congruence half factorial domain (CHFD) of order r if and only if there exists an integer $r>1$ such that if $\prod_{i=1}^{n} x_i = \prod_{j=1}^{m} y_j$ with all the x_i and y_j irreducible, then $n \equiv m \pmod{r}$.

Clearly a unique factorization domain is a half factorial domain, and a half factorial domain is a congruence half factorial domain of order r for all $r>1$. Not all Dedekind domains are CHFD as we will show in Theorem 7. Indeed, we will show for the rings of algebraic integers in a finite number field over the rationals that HFD and CHFD for some $r>1$ are equivalent. We first exhibit a large class of Dedekind domains which are CHFD for some $r>1$ but not HFD.

In questions related to the counting of the number of irreducible factors in a factorization in a Dedekind domain, those irreducibles which generate principal prime ideals always behave well due to the unique factorization of ideals in the Dedekind setting. That is, if $\gamma = \alpha_1 \cdots \alpha_k = \beta_1 \cdots \beta_t$ represents two factorizations of γ into irreducibles, the number of α_i which generate principal primes is the same as the number of β_i which generate principal primes. Thus for the following discussion we can usually assume without loss that the factorizations are produced only by irreducibles that do not generate prime ideals.

Suppose n is a positive integer greater than 3. Let D be a Dedekind domain with class group $\mathbb{Z}_n$ such that all the nonprincipal prime ideals of D are distributed in the ideal classes determined by 1 and $n-1$. The existence of such a domain is guaranteed by results of Claborn [2, 3], and Grams [6]. We begin with the following observation on nonprime irreducible elements of D.

LEMMA 1. *If α is a nonprime irreducible of D, then the principal ideal generated by α falls into one of the following three categories for (not necessarily distinct) nonprincipal prime ideals $\{P_i\}_{i=1}^{n}$ and $\{Q_j\}_{j=1}^{n}$ of D:*

1. $(\alpha) = P_1 \cdots P_n$, *where each P_i is in the class* 1.

2. $(\alpha) = Q_1 \cdots Q_n$, *where each* Q_i *is in the class* $n-1$.

3. $(\alpha) = P_1 Q_1$, *where* P_1 *is in the class* 1 *and* Q_1 *in the class* $n-1$.

Proof. Let α be as given. Consider $(\alpha) = M_1 \cdots M_k$, where each M_i is a nonprincipal prime ideal of D. Suppose each M_i is of class 1. Since the class group of D is $\mathbb{Z}_n$, $k \geqslant n$. Suppose $k > n$. Then since $M_1 \cdots M_n = (\delta)$ for some irreducible δ, δ divides α. Since α is irreducible, $M_{n+1} \cdots M_k = D$ implies that each $M_i = D$ for $i > n$. Thus $k = n$. A similar argument works if all the M_i are assumed to be of class $n-1$. Now, assume that the product $M_1 \cdots M_k$ contains prime ideals of both classes. Let P be a prime of class 1 in this product and Q a prime of class $n-1$. Then $PQ = (\delta)$ for δ some irreducible and an argument similar to that used in the first case completes the proof. ∎

We will refer to a nonprime irreducible of D as being of type 1, 2, or 3 according to the category into which it falls in Lemma 1. In Theorem 4 below we show that D is a CHFD of order $n-2$. In the following two Lemmas and Theorem 4, let elements of the form α_i or α_i', β_j or β_j', θ_k or θ_k' represent irreducible elements of types 1, 2, and 3, respectively.

LEMMA 2. *Let* δ *be a nonzero nonunit of* D. *Suppose* $\delta = \mu_1 \cdots \mu_t = \nu_1 \cdots \nu_s$, *where* $\mu_1, \ldots, \mu_t, \nu_1, \ldots, \nu_s$ *are irreducibles of type* 1 *or* 3. *Then* $t = s$. *The same is true if the irreducibles are of type* 2 *or* 3.

Proof. We argue the lemma assuming the irreducibles are all of type 1 or 3. The argument for type 2 or 3 is similar. Let m and m' be the numbers of type 1 irreducibles in $\mu_1 \cdots \mu_t$ and $\nu_1 \cdots \nu_s$, respectively. In a similar manner let q and q' represent the number of irreducibles of type 3 in each factorization. By observing that the number of prime ideals in the class $n-1$ which appear in each factorization in unique, we see that $q = q'$. Then, counting prime ideals in the class 1, we have $nm + q = nm' + q'$. Thus $m = m'$ and hence $t = s$. ∎

LEMMA 3. *Suppose* δ *is a nonzero nonunit of* D *that has an irreducible factorization with factors of types* 1 *and* 3 *and another with factors of types* 2 *and* 3. *Then both factorizations have factors entirely of type* 3.

Proof. Suppose $\delta = \alpha_1 \cdots \alpha_s \theta_1 \cdots \theta_t = \beta_1 \cdots \beta_r \theta_1' \cdots \theta_q'$. By counting the numbers of prime ideals in class 1 and in class $n-1$ in each factorization we see that $sn + t = q$ and $rn + q = t$. Thus $sn + rn + q = q$ and hence $n(r+s) = 0$. Therefore $r = 0$ and $s = 0$. ∎

THEOREM 4. *Let* D *be a Dedekind domain with class group* $\mathbb{Z}_n$ *with* $n \geqslant 3$ *and all its nonprincipal prime ideals distributed in the classes determined by* 1 *and* $n-1$. *The domain* D *is not a HFD but is a CHFD of order* $n-2$.

Proof. D is not a HFD since the set of elements of $\mathbb{Z}_n$ which contain prime ideals includes 1 and an element of $\mathbb{Z}_n$ which does not divide n (see Zaks [12]). To prove that D is a CHFD of order $n-2$, let δ be a nonzero nonunit of D. If $\delta = \mu_1 \cdots \mu_s$ with all the μ_i irreducible of type 1 (or type 2) then the number of factors which appear is obviously constant. So suppose two factorizations of δ are given,

$$\delta = \alpha_1 \cdots \alpha_r \beta_1 \cdots \beta_s \theta_1 \cdots \theta_t, \tag{1}$$

$$\delta = \alpha'_1 \cdots \alpha'_a \beta'_1 \cdots \beta'_b \theta'_1 \cdots \theta'_c, \tag{2}$$

for $r, s, t, a, b,$ and c nonnegative integers. We assume $r \geqslant s$ as a similar argument will handle the other case. By regrouping irreducibles and the prime factors

$$(P_1 \cdots P_m)(Q_1 \cdots Q_m) = (P_1 Q_1) \cdots (P_m Q_m),$$

(1) can be rewritten as

$$\delta = u\alpha_{s+1} \cdots \alpha_r \mu_1 \cdots \mu_{sn} \theta_1 \cdots \theta_t \tag{1}'$$

where the μ_i are irreducibles of type 3. Thus δ has a representation as discussed in Lemmas 2 and 3 and $a \geqslant b$. Reducing (2) in a similar manner, we have

$$\delta = u\alpha'_{b+1} \cdots \alpha'_a v_1 \cdots v_{bn} \theta'_1 \cdots \theta'_c. \tag{2}'$$

Thus, by Lemma 2,

$$(a-b) + bn + c = (r-s) + sn + t \quad \Rightarrow$$

$$(a+b+c) + b(n-2) = (r+s+t) + s(n-2)$$

and $a+b+c \equiv r+s+t \pmod{n-2}$. ∎

The proof of our next result relies on the fact used by Carlitz in [1] that each ideal class of such a finite algebraic number field over the rationals contains a prime ideal. Further, the proof will rely on the following two lemmas.

LEMMA 5. *Let D be the ring of integers of a finite algebraic number ring K over the rationals with class number 2^k for some $k > 1$. Then D is not a CHFD for any $r > 1$.*

Proof. First, suppose the class group of D is isomorphic to $\sum_{i=1}^{n} \mathbb{Z}_2$ for some positive integer $n > 1$. Let e be the indentity of G. Suppose $a, b,$ and c are elements of G such that $c = a \cdot b$ and neither $a, b,$ nor c is the identity.

Let P, Q, and R be prime ideals of classes, a, b, and c, respectively. It is easy to verify that the ideals P^2, Q^2, R^2, and PQR are all principal generated by an irreducible. Let $P^2=(\alpha)$, $Q^2=(\beta)$, $R^2=(\gamma)$, and $PQR=(\delta)$. Then $\delta^2=u\alpha\beta\gamma$ for some unit u and thus $2\equiv 3 \pmod r$ implies $r=1$.

Now, suppose the class group contains a copy of $\mathbb{Z}_{2^k}$ for some integer $k>1$. Let P be a prime ideal of class 1, Q a prime ideal of class 2^{k-1}, and R a prime ideal of class 2^k-1. Thus the product

$$P^{2^{k-1}}QR^{2^k} \tag{3}$$

is principal as are the products $P^{2^{k-1}}Q$, R^{2^k}, PR, and $QR^{2^{k-1}}$. As above, it is easy to verify that the latter 4 products are each generated by an irreducible element. Let α, β, γ, and δ be generators for these ideals listed in order. The product (3) implies that $\alpha\beta=u\gamma^{2^{k-1}}\delta$ for some unit u. Thus 2 irreducibles can be factored as $2^{k-1}+1$. If D were a CHFD then $2\equiv 2^{k-1}+1 \pmod r$ for some $r>1$. Thus $2^{k-1}-1\equiv 0 \pmod r$ and since r divides an odd number, r itself must be odd.

Now let y be an element of $\mathbb{Z}_{2^k}$ of order 4 and let P be a prime ideal of this class. Let Q be a prime ideal of class containing P^{-1} in $\mathbb{Z}_{2^k}$. Then the ideals P^4, Q^4, and PQ are all principal and generated by an irreducible. If α, β, and γ are these irreducibles in order, then $\alpha\beta=u\gamma^4$ for u a unit. Thus 2 irreducibles can be factored as 4 and $2\equiv 4 \pmod r$ implies $2\equiv 0 \pmod r$. Since r is odd, r must be one. ∎

LEMMA 6. *Let D be a Dedekind domain whose class group has a subgroup isomorphic to $\mathbb{Z}_{p^k}$ for p an odd prime and k any positive integer. If the ideal classes determined by 1 and 2 in $\mathbb{Z}_{p^k}$ both contain prime ideals, then D is not a CHFD for any $r>1$.*

Proof. Let D be a domain as above. Let Q be a prime ideal of the class determined by 1 and R a prime ideal of the class determined by 2 in $\mathbb{Z}_{p^k}$. Then $Q^{p^k}=(\alpha)$ and $R^{p^k}=(\beta)$ are both principal ideals generated by an irreducible. Let $d=(p^k-1)/2$. Then $p^k=2d+1$ and

$$Q^{p^k}R^{p^k}=Q^{p^k}R^{2d+1}=(QR^d)^2(Q^{p^k-2}R). \tag{4}$$

The ideals $QR^d=(\gamma)$ and $Q^{p^k-2}R=(\delta)$ are also principal generated by an irreducible. Thus (4) implies $\alpha\beta=u\gamma^2\delta$ for some unit u. An argument similar to that used in the proof of Lemma 5 completes the proof. ∎

THEOREM 7. *Let D be the ring of integers of a finite algebraic number field K over the rationals. Then K has class number less than or equal to two if and only if D is a CHFD for some $r>1$. Hence, for such rings, CHFD for some $r>1$ and HFD are equivalent.*

Proof. Since HFD implies CHFD for all $r>1$ one of the implications is trivial. For the other, suppose K has class number h greater than two. The proof considers two cases.

(i) If $h=2^k$ for some integer $k>1$ then D is not a CHFD by Lemma 5.

(ii) If $h\neq 2^k$ for some positive k then the class group of D contains a copy of $\mathbb{Z}_{p^m}$ for some odd prime p and positive integer m. Thus D is not a CHFD for any $r>1$ by Lemma 6. ∎

Note that the effect of Theorem 7 is that for the rings of integers of finite extensions of the rationals, CHFD for any $r>1$ implies CHFD for every $r>1$ (which is of course equivalent to HFD). Theorem 4 shows this is not true for general Dedekind domains. However, if we turn our attention in this direction, the proof of Theorem 7 leads us to this interesting result concerning Dedekind domains of class number $\leqslant 3$.

THEOREM 8. *Let D be a Dedekind domain with finite class number $h\leqslant 3$. Then D is a HFD if and only if D is a CHFD for some $r>1$.*

Proof. Again, one of the assertions is trivial. For the other, if $h\leqslant 2$ then D is a HFD by the results of [1]. Thus we need only examine the case when $h=3$. In this case D has class group $\mathbb{Z}_3$. By Lemma 6, if each nonprincipal ideal class contains a prime ideal, then D is not a CHFD for any $r>1$. Thus if D is a CHFD for some $r>1$ all the nonprincipal primes are in one ideal class. By a result of Zaks [11] D is a HFD. ∎

ACKNOWLEDGMENT

The authors express appreciation to Professor Robert Gilmer for discussions related to this work.

REFERENCES

1. L. CARLITZ, A characterization of algebraic number fields with class number two, *Proc. Amer. Math. Soc.* **11** (1960), 391–392.
2. L. CLABORN, Every abelian group is a class group, *Pacific. J. Math.* **18** (1966), 219–222.
3. L. CLABORN, Specified relations in the ideal group, *Michigan Math. J.* **15** (1968), 249–255.
4. A. CZOGALA, Arithmetic characterization of algebraic number fields with small class number, *Math. Z.* **176** (1981), 247–253.
5. F. DIFRANCO AND F. PACE, Arithmetical characterization of rings of algebraic integers with class number three and four, *Boll. Un. Mat. Ital. D(6)* **4** (1985), 63–69.
6. A. GRAMS, The distribution of prime ideals of a Dedekind domain, *Bull. Austral. Math. Soc.* **11** (1974), 429–441.

7. J. KACZOROWSKI, A pure arithmetical characterization for certain fields with a given class group, *Colloq. Math.* **45** (1981), 327–330.
8. U. KRAUSE, A characterization of algebraic number fields with cyclic class group of prime power order, *Math. Z.* **186** (1984), 143–148.
9. D. RUSH, An arithmetic characterization of algebraic number fields with a given class group, *Math. Proc. Cambridge Philos. Soc.* **94** (1983), 23–28.
10. L. SALCE AND P. ZANARDO, Arithmetical characterization of rings of algebraic integers with cyclic ideal class group, *Boll. Un. Mat. Ital. D(6)* **1** (1982), 117–122.
11. J. SLIWA, Factorizations of distinct lengths in algebraic number fields, *Colloq. Math.* **31** (1976), 399–417.
12. A. ZAKS, Half factorial domains, *Israel J. Math.* **37** (1980), 281–302.
13. A. ZAKS, Half factorial domains, *Bull. Amer. Math. Soc.* **82** (1976), 721–723.